BOLETÍN DE ALERTA

Boletín Nro.: 2023-25
Fecha de publicación: 25/05/2023

Tema: Vulnerabilidad crítica en el módulo *mod_proxy* de Apache *HTTP Server.*

Las versiones afectadas son:

- Apache *HTTP* Server, versiones 2.4.0 a 2.4.55.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre una vulnerabilidad que afecta a Apache *HTTP* Server, que permitiría a un atacante obtener acceso no autorizado, realizar ataques del tipo *cache poisoning y request smuggling HTTP* en el sistema afectado. Actualmente para esta vulnerabilidad existe prueba de concepto (*PoC*) pública.

La vulnerabilidad identificada como CVE-2023-25690, de severidad "Crítica" y con puntuación asignada de 9.8. Esta vulnerabilidad se debe a una falla de seguridad en el módulo *mod_proxy* de Apache *HTTP* Server. Para que la aplicación se vea afectada se deben cumplir varios factores tales como:

- La aplicación debe ejecutarse en una versión vulnerable de Apache HTTP Server (v2.4.55 o anterior).
- La configuración del servidor Apache debe tener habilitado el parámetro *RewriteRule* que copia los datos en la cadena de consulta de una *URL* de proxy.
- La aplicación debe tratar al proxy como un límite de seguridad significativo.

Esto permitiría a un atacante remoto a través del envío de direcciones *URLs proxyRewriteRule* especialmente diseñadas obtener acceso no autorizado al servidor *proxy*, realizar ataques del tipo *cache poisoning* y *request smuggling HTTP* en el sistema afectado.

Impacto:

La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener acceso no autorizado al servidor.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante en el siguiente enlace:

- https://httpd.apache.org/download.cgi#apache24.

Información adicional:

- https://attackerkb.com/topics/0Uka1VHsPO/cve-2023-25690/rapid7-analysis?referrer=notificationEmail

- https://nvd.nist.gov/vuln/detail/CVE-2023-25690
- https://www.cert.gov.py/noticias/vulnerabilidades-de-cross-site-scripting-xss-y-request-smuggling-http-en-apache-http-server/
- https://httpd.apache.org/security/vulnerabilities_24.html#:~:text=HTTP%20request%20splitting%20with%20mod_rewrite%20and%20mod_proxy
- https://httpd.apache.org/download.cgi#apache24